Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 125 (2007) 442–458

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

On Galois structure of the integers in elementary abelian extensions of local number fields

Yoshimasa Miyata

Faculty of Education, Shizuoka University, Shizuoka 422-8529, Japan

Received 12 October 2005; revised 17 October 2006

Available online 28 December 2006

Communicated by David Goss

Abstract

Let p be an odd prime number and k a finite extension of $\mathbb{Q}_p$. Let K/k be a totally ramified elementary abelian Kummer extension of degree p^2 with Galois group G. We determine the isomorphism class of the ring of integers in K as an $\mathfrak{o}G$-module under some assumptions. The obtained results imply there exist extensions whose rings are $\mathbb{Z}_pG$-isomorphic but not $\mathfrak{o}G$-isomorphic, where $\mathbb{Z}_p$ is the ring of p-adic integers. Moreover we obtain conditions that the rings of integers are free over the associated orders and give extensions whose rings are not free.

Keywords: Local fields; Free module; Isomorphism class; Invariant factor

0. Introduction

Let p be an odd prime number. Let k be a $\mathfrak{p}$-adic number field and assume k contains a primitive pth root of unity. Let $\mathfrak{o}$ be the ring of integers of k and π be a prime element. Let G be an elementary abelian group of order p^2 and K/k be a totally ramified extension with Galois group G. Then the ring $\mathfrak{O}_K$ of integers in K is an $\mathfrak{o}G$-module and a $\mathbb{Z}_pG$-module. Elder and Madan [3] determined the decomposition of $\mathfrak{O}_K$ into indecomposable $\mathbb{Z}_pG$-modules for the extension K/k whose first ramification number is 1. Let K'/k be another extension with Galois group G. From their results, we know that if extensions K and K' have the same ramification numbers, then two decompositions of $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$ into indecomposable $\mathbb{Z}_pG$-modules are the

E-mail address: ecymiya@ipc.shizuoka.ac.jp.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.12.005

same. In this paper, we obtain necessary and sufficient conditions for $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$ to be $\mathfrak{o}G$-isomorphic under certain assumptions (Theorem 3 in Section 2), from which we see there exist extensions such that $\mathfrak{O}_K$ and $\mathfrak{O}_{K'}$ are $\mathbb{Z}_pG$-isomorphic but not $\mathfrak{o}G$-isomorphic.

Let $\mathfrak{A}_K$ be the ring of $\mathfrak{o}G$-endomorphisms of $\mathfrak{O}_K$. Byott [1] proved there exist Galois extensions K of degree p^2 whose rings $\mathfrak{O}_K$ are $\mathfrak{A}_K$-free modules. In the previous paper [6], we obtained conditions for $\mathfrak{O}_K$ to be $\mathfrak{A}_K$-free for cyclic Kummer extensions K. In this paper, we obtain the similar conditions (Theorem 4 in Section 3) and show $\mathfrak{O}_K$ is not $\mathfrak{A}_K$-free for elementary abelian extensions K satisfying certain assumptions (Theorem 5 in Section 3).

Finally we mention results stated in Section 1. We first deal with Kummer extensions L of degree p and recall the fact that if the first ramification numbers $c_1(L/k)$ are equal, then the rings $\mathfrak{O}_L$ are isomorphic (Theorem 1). Next we deal with elementary abelian Kummer extensions of degree p^2. Let α and β be Kummer elements of $\mathfrak{O}_K$ with $K = k(\alpha, \beta)$ and $\mathfrak{o}[\alpha, \beta]$ be the order generated by α and β in $\mathfrak{O}_K$. Then we obtain the invariant factors of $\mathfrak{o}[\alpha, \beta]$ in $\mathfrak{O}_K$ for extensions K satisfying some properties (Theorem 2).

1. Invariant factor

We first recall the results about Galois module structure of rings $\mathfrak{O}_L$ of Kummer extensions L of degree p. Let val_k denote the valuation of k and $e_0 = \mathrm{val}_k(p)/(p-1)$. Let $c = c(L/k)$ be the first ramification number of a totally ramified extension L. As is well known, $1 \leqslant c < pe_0$ and $(c, p_0) = 1$ or $c = pe_0$. By Wyman's results [8, Corollary 13], there exists a Kummer element α satisfying $\mathrm{val}_L(\alpha - 1) = pe_0 - c$ for $c < pe_0$ or $\mathrm{val}_L(\alpha) = 1$ for $c = pe_0$. Let $d_i = [\mathrm{val}_L((\alpha-1)^i)/p]$ for the one-unit α, where $[x]$ denotes an integer n with $n \leqslant x < n+1$. As $(\mathrm{val}_L(\alpha - 1), p) = 1$, we have

$$\mathfrak{O}_L = \sum_{0 \leqslant i < p} \mathfrak{o}(\alpha - 1)^i/\pi^{d_i}. \tag{1}$$

We observe $d_i = 0$ for $1 \leqslant i < p$ if and only if $\mathrm{val}_L(\alpha - 1) = 1$, that is, $c = pe_0 - 1$. Then

$$\mathfrak{O}_L = \sum_i \mathfrak{o}(\alpha-1)^i = \sum_i \mathfrak{o}\alpha^i.$$

For $\mathrm{val}_L(\alpha) = 1$, of course, $\mathfrak{O}_L = \sum_i \mathfrak{o}\alpha^i$. Let L' be a totally ramified extension of degree p with $G = Gal(L'/k)$. Then by (1), we have immediately the following results (cf. [4, p. 159, Theorem 1]).

Theorem 1. *Let L' and L be totally ramified Kummer extensions of degree p. Then $\mathfrak{O}_{L'} \cong \mathfrak{O}_L$ as $\mathfrak{o}G$-modules if and only if $c(L'/k) = c(L/k)$, or $c(L'/k) = pe_0 - 1$ and $c(L/k) = pe_0$ (or $c(L'/k) = pe_0$ and $c(L/k) = pe_0 - 1$).*

Next let K/k be a totally ramified elementary abelian Kummer extension of degree p^2 as in Introduction. Let $c_1 = c_1(K/k)$ be the first ramification number of K/k. We note $1 \leqslant c_1 < pe_0$ and $(c_1, p) = 1$, because K/k is a cyclic extension of degree p^2 if $c_1 = pe_0$ (cf. [7, p. 72]). Let G_2 be the (c_1+1)th ramification group. Let $K_1 = K^{G_2}$ in case G_2 is not a trivial group $\{1\}$, and K_1 be an arbitrary subextension of degree p in K in case $G_2 = \{1\}$. Let α be a Kummer element of K_1 with $\mathrm{val}_{K_1}(\alpha - 1) = pe_0 - c_1$ and β be another Kummer element with $k(\alpha, \beta) = K$. Then

we can choose β such that $\mathrm{val}_K(\alpha-1) \geqslant \mathrm{val}_K(\beta-1) = p(pe_0 - c_1(k(\beta)/k))$ in case β is a one-unit. By $G_2 = Gal(K/k(\alpha))$ or $G_2 = \{1\}$, we see $c_1(K/k(\beta)) = c_1(K/k)$ and there is a one-unit γ of K such that $\gamma^p \in k(\beta)$ and $\mathrm{val}_K(\gamma-1) = p^2e_0 - c_1(K/k)$. Then for some one-unit U of $k(\beta)$, $\alpha = U\gamma$ and $\alpha - 1 = U - 1 + U(\gamma-1)$ with $\mathrm{val}_K(U(\gamma-1)) = p^2e_0 - c_1$. By $(c_1, p) = 1$, we have $(\mathrm{val}_K(U(\gamma-1)), p) = 1$ and $\mathrm{val}_K(\alpha-1) = \mathrm{val}_K(U-1)$. By (1), in case β is a one-unit, for some element a'_i of $\mathfrak{o}$ for $0 \leqslant i < p$,

$$U - 1 = \sum_i a'_i(\beta-1)^i/\pi^{d'_i}, \tag{2}$$

where $d'_i = [\mathrm{val}_K(\beta-1)^i/p^2]$. Similarly in case $\mathrm{val}_K(\beta) = p$, we have also, for some a_i of $\mathfrak{o}$,

$$U - 1 = \sum_i a_i\beta^i.$$

We define an element f of $\mathfrak{O}$ by $f = \alpha - 1 - (U-1)$, and integers d_{pi+j} by $d_{pi+j} = [\mathrm{val}_K(f^i(\beta-1)^j)/p^2]$ ($d_{pi+j} = [\mathrm{val}_K(f^i\beta^j)/p^2]$) for $0 \leqslant i, j < p$ in case β is a one-unit (a prime element), respectively. Then, recalling $(\mathrm{val}_K(U(\gamma-1)), p) = 1$, we have immediately the next proposition.

Proposition 1. *Let K/k be as above. Then in case $\mathrm{val}_K(\beta-1) > 0$, $\mathfrak{O}_K = \sum_{0\leqslant i,j<p} \mathfrak{o} f^i(\beta-1)^j/\pi^{d_{pi+j}}$, and in case $\mathrm{val}_K(\beta) = p$, $\mathfrak{O}_K = \sum_{i,j} \mathfrak{o} f^i\beta^j/\pi^{d_{pi+j}}$.*

Theorem 2. *Let K/k be a totally ramified elementary abelian Kummer extension of degree p^2 and let α, β be Kummer elements as above. In case β is a one-unit, assume $(p-1)\mathrm{val}_K(\beta-1) \leqslant \mathrm{val}_K(\alpha-1)$. a'_i is an element of $\mathfrak{o}\pi^{d_i}$ and a set $\{\pi^{d_{pi+j}} \mid 0 \leqslant i, j < p\}$ is the invariant factors of the order $\mathfrak{o}[\alpha,\beta]$ in $\mathfrak{O}_K$.*

Proof. In case β is a one-unit, for $j \neq j'$, $\mathrm{val}_K(\beta-1)^j \not\equiv \mathrm{val}_K(\beta-1)^{j'} \pmod{p^2}$, so for some i_0, $\mathrm{val}_K(U-1) = \mathrm{val}_K(a'_{i_0}(\beta-1)^{i_0}/\pi^{d'_{i_0}})$ and $\mathrm{val}_K(a'_i(\beta-1)^i/\pi^{d'_i}) > \mathrm{val}_K(a'_{i_0}(\beta-1)^{i_0}/\pi^{d'_{i_0}})$ for $i \neq i_0$. By $\mathrm{val}_K(\alpha-1) = \mathrm{val}_K(U-1)$ and the assumption,

$$\begin{aligned} i\,\mathrm{val}_K(\beta-1) + \mathrm{val}_K\left(a'_i/\pi^{d'_i}\right) &> i_0\,\mathrm{val}_K(\beta-1) + \mathrm{val}_K\left(a'_{i_0}/\pi^{d'_{i_0}}\right) \\ &= \mathrm{val}_K(\alpha-1) \\ &\geqslant (p-1)\,\mathrm{val}_K(\beta-1), \end{aligned}$$

so $\mathrm{val}_K(a'_i/\pi^{d'_i}) \geqslant 0$. The first part of Theorem 2 is proved. The second part immediately follows from Proposition 1. □

2. Isomorphism classes

Let K/k, α, β be as above. Throughout this section, we assume $\mathrm{val}_K(\beta) = p$ and $\mathrm{val}_K(\alpha-1) = p^2e_0 - p$. Then $c_1(k(\alpha)/k) = 1$ and $c_1(k(\beta)/k) = pe_0$. We seek an element f such as stated in Section 1. As $\mathrm{val}_K(\alpha-1) \equiv p(p-1) \pmod{p^2}$, we can take an element a of $\mathfrak{o}$ with $\mathrm{val}_K(\alpha - 1 - a\beta^{p-1}) > \mathrm{val}_K(\alpha-1)$. Then $\alpha - 1 - a\beta^{p-1} = U - 1 - a\beta^{p-1} + U(\gamma-1)$

and $(\mathrm{val}_K(U(\gamma-1)),p)=1$ because $\mathrm{val}_K(U(\gamma-1))=p^2e_0-c_1(K/k)=p^2e_0-1$. Therefore $\mathrm{val}_K(\alpha-1-a\beta^{p-1})=\min\{\mathrm{val}_K(U-1-a\beta^{p-1}),\mathrm{val}_K(\gamma-1)\}$, whence $\mathrm{val}_K(U-1-a\beta^{p-1})>p^2e_0-p$. As p divides $\mathrm{val}_K(U-1-a\beta^{p-1})$, it follows $\mathrm{val}_K(U-1-a\beta^{p-1})\geqslant p^2e_0$, by which

$$\mathrm{val}_K\bigl(\alpha-1-a\beta^{p-1}\bigr)=\mathrm{val}_K(\gamma-1)=p^2e_0-1.$$

Hence we can put $f=\alpha-1-a\beta^{p-1}$. Since $\mathrm{val}_K(\alpha-1)=\mathrm{val}_K(a\beta^{p-1})$, we have

$$\mathrm{val}_k(a)=e_0-1\quad\text{and}\quad a=a_0\pi^{e_0-1},\tag{3}$$

where a_0 is in the fixed multiplicative system of representatives of the residue field $\mathfrak{o}/(\pi)$. As in Section 1, let d_{pi+j} be defined by

$$d_{pi+j}=\bigl[\mathrm{val}_K\bigl(\bigl(\alpha-1-a\beta^{p-1}\bigr)^i\beta^j\bigr)/p^2\bigr].\tag{4}$$

Define a function δ_n of integers n by

$$\delta_n=1\quad\text{if } n>0\quad\text{and}\quad\delta_n=0\quad\text{if } n\leqslant 0.$$

Denote the remainder on dividing n by p by $r(n)$ $(0\leqslant r(n)<p)$. Then from (4), we can easily prove

Lemma 1. *For* $0<i,j<p$, $d_{pi+j}=ie_0-\delta_{1-j}$.

Let σ and τ be generators of G such that $K^{\langle\tau\rangle}=k(\alpha)$ and $K^{\langle\sigma\rangle}=k(\beta)$. Let θ be a primitive pth root of unity. We have $\sigma(\alpha^i\beta^j)=\theta^i\alpha^i\beta^j$ and $\tau(\alpha^i\beta^j)=\theta^j\alpha^i\beta^j$, replacing σ and τ if necessary. Let K'/k be another elementary abelian extension of degree p^2 with $Gal(K'/k)=G$. Let α' and β' be Kummer elements with $k(\alpha')=(K')^{\langle\tau\rangle}$ and $k(\beta')=(K')^{\langle\sigma\rangle}$. We seek the conditions $\mathfrak{O}_{K'}\cong\mathfrak{O}_K$. Assume there exist an $\mathfrak{o}G$-isomorphism $\Phi:\mathfrak{O}_{K'}\to\mathfrak{O}_K$. We may assume $\Phi(1)=1$. Then $\mathfrak{O}_{k(\alpha')}\cong\mathfrak{O}_{k(\alpha)}$ and $\mathfrak{O}_{k(\beta')}\cong\mathfrak{O}_{k(\beta)}$. By Theorem 1, we take α' with $\mathrm{val}_{K'}(\alpha'-1)=p^2e_0-p$ and also β' with $\mathrm{val}_{K'}(\beta'-1)=p$ or $\mathrm{val}_{K'}(\beta')=p$. Let $\sigma(\alpha')=\theta^{i_0}\alpha'$, then for i_0' with $i_0'i_0\equiv 1 \pmod p$, $\sigma((\alpha')^{i_0'})=\theta\alpha'^{i_0'}$ and so $\mathrm{val}_{K'}((\alpha')^{i_0'}-1)=p^2e_0-p$ clearly. Replace α' by $(\alpha')^{i_0'}$, which is denoted by the same character α' again. Then we have $\sigma(\alpha')=\theta\alpha'$. Let $\tau(\beta')=\theta^{j_0}\beta'$, then $\Phi(\mathfrak{o}\beta')=\mathfrak{o}\beta^{j_0}$ because Φ is an $\mathfrak{o}G$-isomorphism. Moreover $\Phi(\mathfrak{o}(\alpha')^i(\beta')^j)=\mathfrak{o}\alpha^i\beta^{r(j_0j)}$ and so there exist units u_{pi+j} of $\mathfrak{o}$ with $\Phi((\alpha')^i(\beta')^j)=u_{pi+j}\alpha^i\beta^{r(j_0j)}$, whence $\Phi(\sum_{0\leqslant i,j<p}\mathfrak{o}(\alpha')^i(\beta')^j)=\sum_{i,j}\mathfrak{o}\alpha^i\beta^j$.

Proposition 2. *If* $\mathfrak{O}_{K'}\cong\mathfrak{O}_K$, *then* (i) $\mathrm{val}_{K'}(\beta')=p$ *and* (ii) $j_0=1$.

Proof. As $\mathrm{val}_K(\alpha-1)=p^2e_0-p$, $(\alpha-1)\beta\equiv 0 \pmod{\pi^{e_0}\mathfrak{O}_K}$. Let $\Phi^{-1}(\alpha\beta)=u_1'\alpha'(\beta')^j$ and $\Phi^{-1}(\beta)=u_0'(\beta')^j$. Suppose $\mathrm{val}_K(\beta'-1)>0$. As $\pi^{e_0}\Phi(\mathfrak{O}_{K'})=\pi^{e_0}\mathfrak{O}_K$,

$$u_1'\alpha'(\beta')^j-u_0'(\beta')^j\equiv 0\quad\bigl(\mathrm{mod}\,\pi^{e_0}\mathfrak{O}_{K'}\bigr),$$

so $u_1'(\alpha'-1)(\beta')^j+(u_1'-u_0')(\beta')^j\equiv 0 \pmod{\pi^{e_0}}$. Since $\mathrm{val}_K(\alpha'-1)\not\equiv 0 \pmod{p^2}$, $u_1'(\alpha'-1)\equiv 0 \pmod{\pi^{e_0}}$, so $u_1'\equiv 0 \pmod{\pi}$, a contradiction, which completes the proof

of (i). By (i), we have $\mathrm{val}_{K'}(\beta') = p$. Then similarly as for K, there exists some unit a' of $\mathfrak{o}$ with $\mathrm{val}_{K'}(\alpha' - 1 - a'(\beta')^{p-1}) = p^2 e_0 - 1$. Then $(\alpha' - 1 - a'(\beta')^{p-1})^2 \beta' \equiv 0 \pmod{\pi^{2e_0}\mathfrak{O}_{K'}}$. Hence

$$u_{2p+1}\alpha^2\beta^{j_0} - 2u_{p+1}\alpha\beta^{j_0} + u_1\beta^{j_0} - 2a'u_p(\beta')^p\alpha + 2a'(\beta')^p + (a')^2(\beta')^p u_{p-1}\beta^{p-j_0} \equiv 0 \quad \big(\mathrm{mod}\ \pi^{2e_0}\mathfrak{O}_K\big).$$

As $\alpha = 1 + a\beta^{p-1} + U(\gamma - 1)$,

$$\begin{aligned} &u_{2p+1}\big(1 + a\beta^{p-1} + U(\gamma-1)\big)^2\beta^{j_0} - 2u_{p+1}\big(1 + a\beta^{p-1} + U(\gamma-1)\big)\beta^{j_0} + u_1\beta^{j_0} \\ &\quad - 2a'(\beta')^p u_p\big(1 + a\beta^{p-1} + U(\gamma-1)\big) + 2a'(\beta')^p + (a')^2(\beta')^p u_{p-1}\beta^{p-j_0} \\ &\equiv 0 \quad \big(\mathrm{mod}\ \pi^{2e_0}\mathfrak{O}_K\big). \end{aligned}$$

Suppose $j_0 > 1$. Since $\mathrm{val}_K(U(\gamma-1)\beta^{p-1+j_0}) \not\equiv \mathrm{val}_K(U(\gamma-1)) \pmod{p^2}$, $2a'(\beta')^p \times u_p U(\gamma-1)$ is the only term whose valuation is congruent to $\mathrm{val}_K U(\gamma-1)$ with respect to the modulus p^2. Then

$$2a'(\beta')^p u_p U(\gamma-1) \equiv 0 \quad \big(\mathrm{mod}\ \pi^{2e_0}\big).$$

By $p \neq 2$, $u_p \equiv 0 \pmod{\pi}$, which is a contradiction. Hence $j_0 = 1$. □

In the following, for brevity, identify β^p with a prime element π of $\mathfrak{o}$ and denote a' by b. Let $(\beta')^p = v\pi$ and $v = v_0^p v'$ such that $v' \equiv 1 \pmod{\pi}$ and v_0^p is an element of multiplicative representatives of $\mathfrak{o}/(\pi)$. Let $\beta'' = v_0^{-1}\beta'$, then $(\beta'')^p = v'\pi$ and $\alpha' - 1 - b(\beta')^{p-1} = \alpha' - 1 - bv_0^{p-1}(\beta'')^{p-1}$. Denoting β'', v' and bv_0^{p-1} by β', v and b, respectively, we have $(\beta')^p = v\pi$ and

$$v - 1 \in (\pi). \tag{5}$$

We remark that α' and β' satisfy also the equality (4) where α, β and K are replaced by α', β' and K', respectively.

Proposition 3. *$\mathfrak{O}_{K'} \cong \mathfrak{O}_K$ if and only if for $0 \leqslant pi + j < p^2$, there exist units u_{pi+j} of $\mathfrak{o}$ such that*

$$\sum_{0 \leqslant m \leqslant l \leqslant i} \binom{i}{l}\binom{l}{m}(-1)^{i-m}b^{i-l}\pi^{i-l}v^{i-l-\delta_{i-j-l}} \cdot u_{pm+r(j-i+l)}\alpha^m\beta^{j-i+l} \equiv 0 \quad \big(\mathrm{mod}\ \pi^{ie_0-\delta_{1-j}}\big). \tag{6}$$

Proof. First suppose $\mathfrak{O}_{K'} \cong \mathfrak{O}_K$. By Lemma 1 with (3) replacing K by K', for α' and β', we have

$$\big(\alpha' - 1 - b(\beta')^{p-1}\big)^i(\beta')^j \equiv 0 \quad \big(\mathrm{mod}\ \pi^{ie_0-\delta_{1-j}}\mathfrak{O}_{K'}\big).$$

Therefore $\Phi((\alpha' - 1 - b(\beta')^{p-1})^i(\beta')^j) \equiv 0 \pmod{\pi^{ie_0-\delta_{1-j}}\mathfrak{O}_K}$. In case $j - i + l < 0$, $(\beta')^{p(i-l)+j-i+l} = (v\pi)^{i-l-1}(\beta')^{p+j-i+l}$. Thus by $\beta^p = \pi$,

$$\Phi\Bigg(\sum_{0\leqslant m\leqslant l\leqslant i}\binom{i}{l}(-1)^{i-l}\binom{l}{m}(-1)^{l-m}b^{i-l}(\beta')^{p(i-l)}(\alpha')^m(\beta')^{j-i+l}\Bigg)$$
$$\equiv\sum_{0\leqslant m\leqslant l\leqslant i}\binom{i}{l}(-1)^{i-l}\binom{l}{m}(-1)^{l-m}b^{i-l}\pi^{i-l}v^{i-l-\delta_{i-j-l}}$$
$$\cdot u_{pm+r(j-i+l)}\alpha^m\beta^{j-i+l}\equiv 0\pmod{\pi^{ie_0-\delta_{1-j}}}.$$

Hence the congruences (6) hold.

Conversely suppose the above congruences (6) hold. We note

$$\mathfrak{O}_{K'}=\sum_{0\leqslant i,j<p}\mathfrak{o}\big(\alpha'-1-b(\beta')^{p-1}\big)^i(\beta')^j/\pi^{d_{pi+j}}$$

and define an $\mathfrak{o}G$-homomorphism Φ by $\Phi((\alpha')^i(\beta')^j)=u_{pi+j}\alpha^i\beta^j$. Then $\Phi(\mathfrak{o}[\alpha',\beta'])=\mathfrak{o}[\alpha,\beta]$ and $\Phi((\alpha'-1-b(\beta')^{p-1})^i(\beta')^j/\pi^{d_{pi+j}})\in\mathfrak{O}_K$ by Lemma 1 with (6), so $\Phi(\mathfrak{O}_{K'})\subseteq\mathfrak{O}_K$. We have $[\mathfrak{O}_K:\mathfrak{o}[\alpha,\beta]]=\pi^{\sum d_{pi+j}}$ and $[\Phi(\mathfrak{O}_{K'}):\mathfrak{o}[\alpha,\beta]]=\pi^{\sum d_{pi+j}}$, where $[M:N]$ denotes the module index of N in M (cf. [2, Chapter 1]). Hence $\Phi(\mathfrak{O}_{K'})=\mathfrak{O}_K$ and $\mathfrak{O}_{K'}\cong\mathfrak{O}_K$. □

As for K, we can take b_0 for K' satisfying $b=b_0\pi^{e_0-1}$. In the rest of this section, we shall prove that if $\mathfrak{O}_{K'}\cong\mathfrak{O}_K$, then $a_0=b_0$. By $\alpha=1+(\alpha-1)$, $\alpha^m=\sum_{0\leqslant m_0\leqslant m}\binom{m}{m_0}(\alpha-1)^{m_0}$ and by (6) in Proposition 3,

$$\sum_{0\leqslant m_0\leqslant m\leqslant i}\Bigg(\sum_{m\leqslant l\leqslant i}\binom{i}{l}\binom{l}{m}(-1)^{i-m}v^{i-l-\delta_{i-j-l}}(b\pi)^{i-l}u_{pm+r(j-i+l)}\beta^{j-i+l}\Bigg)$$
$$\cdot\binom{m}{m_0}(\alpha-1)^{m_0}\equiv 0\pmod{\pi^{ie_0-\delta_{1-j}}}.$$

As $\alpha-1=a\beta^{p-1}+U(\gamma-1)$,

$$(\alpha-1)^{m_0}=\big(a\beta^{p-1}+U(\gamma-1)\big)^{m_0}=\sum_{0\leqslant m_1\leqslant m_0}\binom{m_0}{m_1}\big(a\beta^{p-1}\big)^{m_1}\big(U(\gamma-1)\big)^{m_0-m_1}.$$

Put $m_2=m_0-m_1$. Then, by $\mathrm{val}_K(\gamma-1)=p^2e_0-1$,

$$\mathrm{val}_K\big(\beta^{j-i+l}\beta^{m_1(p-1)}(\gamma-1)^{m_2}\big)\equiv p(j-i)+p(l-m_1)-m_2\pmod{p^2}.$$

We have immediately the following lemma.

Lemma 2. $\mathrm{val}_K(\beta^{j-i+l'}\beta^{m_1'(p-1)}(\gamma-1)^{m_2'})\equiv\mathrm{val}_K(\beta^{j-i+l}\beta^{m_1(p-1)}(\gamma-1)^{m_2})\pmod{p^2}$ *if and only if* $m_2'=m_2$ *and* $l'-m_1'=l-m_1$.

Let m_2 and $l-m_1$ be fixed and put $n=l-m_1-m_2$, so n is fixed. Then from (6) with $\beta^p=\pi$, it follows that for each i, j,

$$\sum_{0\leqslant m_1\leqslant m_0\leqslant m\leqslant l\leqslant i} \binom{i}{l}\binom{l}{m}(-1)^{i-m}\binom{m}{m_0}\binom{m_0}{m_1} v^{i-l-\delta_{i-j-l}}(b\pi)^{i-l}(a\pi)^{m_1} \cdot u_{pm+r(j-i+l)}\big(U(\gamma-1)\big)^{m_2}\beta^{j-i+l-m_1} \equiv 0 \pmod{\pi^{ie_0-\delta_{1-j}}}, \tag{7}$$

where the sum runs over m_1, m_0, m, l satisfying the equations $l - m_1 = n + m_2$ and $m_0 - m_1 = m_2$. By (3), $a = a_0\pi^{e_0-1}$ and similarly $b = b_0\pi^{e_0-1}$, so $(b\pi)^{i-l}(a\pi)^{m_1} = b_0^{i-l}a_0^{m_1}\pi^{e_0(i-l+m_1)}$. By $m_0 = m_1 + m_2$,

$$\begin{aligned}
&\operatorname{val}_K\big(\pi^{ie_0-\delta_{1-j}}\big) - \operatorname{val}_K\big(\big(U(\gamma-1)\big)^{m_2}\beta^{j-i+l-m_1}\pi^{e_0(i-l+m_1)}\big)\\
&\quad = p^2(ie_0-\delta_{1-j}) - m_2\big(p^2e_0-1\big) - p(j-i+l-m_1) - p^2e_0(i-l+m_1)\\
&\quad = p^2\big(e_0(l-m_0)-\delta_{1-j}\big) - p(j-i+l-m_1) + m_2.
\end{aligned}$$

Put $q = e_0(l-m_0) - \delta_{1-j} + \delta_{-p(j-i+l-m_1)+m_2}$. Therefore, by (7),

$$\sum_{0\leqslant m_1\leqslant m_0\leqslant m\leqslant l\leqslant i} \binom{i}{l}\binom{l}{m}(-1)^{i-m}\binom{m}{m_0}\binom{m_0}{m_1} v^{i-l-\delta_{i-j-l}}b_0^{i-l}a_0^{m_1} \cdot u_{pm+r(j-i+l)} \equiv 0 \pmod{\pi^q}, \tag{8}$$

where the sum runs over m_1, m_0, m, l as in (7). Here take $m_2 = i-1$ and $n = 1$, then $i - m_1 - (i-1) \geqslant l - m_1 - (i-1) = l - m_1 - m_2 = n = 1$, hence $1 - m_1 \geqslant 1$, so $m_1 = 0$ and $m_0 = m_1 + m_2 = i - 1$. By $1 = n = l - m_1 - m_2$, $l = 1 + m_2 = 1 + i - 1 = i$. As $m_0 \leqslant m \leqslant l$, $m = i-1$ or i. In this case, $q = e_0 - 0 + 0$ for $j \geqslant 1$ and $q = e_0 - 1 + 1$ for $j = 0$ with $i \geqslant 2$. Then by (8), for $j \geqslant 1$,

$$\begin{aligned}
&\binom{i}{i}\binom{i}{i-1}(-1)\binom{i-1}{i-1}\binom{i-1}{0}v^0b_0^0a_0^0u_{p(i-1)+j}\\
&\quad + \binom{i}{i}\binom{i}{i}\binom{i}{i-1}\binom{i-1}{0}v^0b_0^0a_0^0u_{pi+j} \equiv 0 \pmod{\pi^{e_0}}.
\end{aligned}$$

Then $u_{pi+j} - u_{p(i-1)+j} \equiv 0 \pmod{\pi^{e_0}}$, hence

$$u_{pi+j} - u_j \equiv 0 \pmod{\pi^{e_0}} \quad \text{for } j \geqslant 1. \tag{9}$$

For $j = 0$ with $i \geqslant 2$, similarly, $u_{pi} - u_{p(i-1)} \equiv 0 \pmod{\pi^{e_0}}$. Now remarking $(\alpha'-1)^2 \equiv 0 \pmod{\pi^{2e_0-1}}$, we have $(\alpha')^2 - 2\alpha' + 1 \equiv 0 \pmod{\pi^{2e_0-1}}$ and so $u_{2p}\alpha^2 - 2u_p\alpha + 1 \equiv 0 \pmod{\pi^{2e_0-1}}$. Then $u_{2p} - 2u_p + 1 \equiv 0 \pmod{\pi^{e_0}}$. By the above congruence, $-u_p + 1 \equiv 0 \pmod{\pi^{e_0}}$, hence

$$u_{pi} - 1 \equiv 0 \pmod{\pi^{e_0}}. \tag{10}$$

Now we treat the case $n = 0$ (with $m_2 = i-1$). Then $l = m_1 + m_2 = m_0$, so $m = m_0$ by $m_0 \leqslant m \leqslant l$. As $i - m_1 - m_2 \geqslant l - m_1 - m_2 = 0$, it follows $1 = i - m_2 \geqslant m_1 \geqslant 0$. For $m_1 = 0$, $l = m = m_0 = i - 1$ and for $m_1 = 1$, $l = m = m_0 = i$. For $j = 1$ and $i \geqslant 2$, $q = e_0(l-m_0) - \delta_{1-j} +$

$\delta_{-p(j-i+l-m_1)+m_2} = 0 - 0 + 1$ by $m_2 = i - 1 > 0$. By (8) and (5), $-b_0 u_{p(i-1)} + a_0 u_{pi+1} \equiv 0 \pmod{\pi}$. Then by (9) and (10),

$$a_0 u_1 \equiv b_0 \pmod{\pi}. \tag{11}$$

Next let $m_2 = i - 2$ and $n = 0$, then $i - m_1 - (i-2) \geqslant l - m_1 - (i-2) = 0$, so $2 \geqslant m_1$ ($\geqslant 0$). For $m_1 = 2$, it follows $l = i, m_0 = i - 2 + 2 = i$ and $m = i$. For $m_1 = 1$, $l = i - 1$, $m_0 = i - 2 + 1 = i - 1$ and $m = i - 1$. For $m_1 = 0, l = i - 2, m_0 = i - 2 + 0 = i - 2$ and $m = i - 2$. In case $j = 1$, $q = e_0(l - m_0) - \delta_{1-j} + \delta_{-p(j-i+l-m_1)+m_2} = 0 - 0 + 1$. As $\binom{i}{m_1+m_2}\binom{m_1+m_2}{m_2} = \binom{i}{m_2}\binom{i-m_2}{m_1}$, $\binom{i}{l}\binom{m_0}{m_1} = \binom{i}{m_0}\binom{m_0}{m_2} = \binom{i}{m_2}\binom{i-m_2}{m_1}$. Then by (8) with (5),

$$\sum_{0 \leqslant m_1 \leqslant 2} \binom{i}{m_2}\binom{i-m_2}{m_1}\binom{m_0}{m_0}\binom{m_0}{m_0}(-1)^{i-m_2-m_1} a_0^{m_1} b_0^{i-m_2-m_1} \cdot u_{r(1-2+m_1)} \equiv 0 \pmod{\pi}.$$

Hence $\binom{2}{2}(-1)^{-2} a_0^2 b_0^{-2} u_1 + \binom{2}{1}(-1) a_0 b_0^{-1} u_0 + \binom{2}{0}(-1)^{-0} u_{p-1} \equiv 0 \pmod{\pi}$. By (10) and (11), $(a_0/b_0) - 2(a_0/b_0) + u_{p-1} \equiv 0 \pmod{\pi}$, so

$$u_{p-1} \equiv a_0/b_0 \pmod{\pi}. \tag{12}$$

We have treated the restricted cases $i - m_2 \leqslant 2$ in the above. In the following we consider the case where m_2 (> 0) is not restricted. Put $m_2' = i - m_2$ and let $n = 0$. As in the above, we have $m_2' \geqslant m_1 \geqslant 0$. By $n = 0$, $l = m_1 + m_2 = m_0$ and $l = m = m_0$. For $1 \leqslant j \leqslant i - m_2$, $q = (l - m_0)e_0 - \delta_{1-j} + \delta_{-p(j-i+l-m_1)+m_2} = 1$. For $j = i - m_2$, $r(j - i + m_2 + m_1) = m_1$. By (8),

$$\sum_{0 \leqslant m_1 \leqslant m_2'} \binom{i}{m_1+m_2}\binom{m_1+m_2}{m_1+m_2}(-1)^{i-m_1-m_2}\binom{m_1+m_2}{m_1+m_2}\binom{m_1+m_2}{m_2} \cdot v^{i-m_1-m_2} a_0^{m_1} u_{m_1} b_0^{i-m_1-m_2} \equiv 0 \pmod{\pi}.$$

As in the case $m_2' = i - m_2 = 2$, we have

$$\sum_{0 \leqslant m_1 \leqslant m_2'} \binom{i-m_2}{m_1}(-1)^{m_1}(a_0/b_0)^{m_1} u_{m_1} \equiv 0 \pmod{\pi}.$$

Using induction on m_2', we prove $u_{m_2'} \equiv (b_0/a_0)^{m_2'} \pmod{\pi}$. For $m_2' = 1$, by (11), the result holds. For $m_1 < m_2'$, assume $u_{m_1} \equiv (b_0/a_0)^{m_1} \pmod{\pi}$, i.e. $u_{m_1}(a_0/b_0)^{m_1} \equiv 1 \pmod{\pi}$. Then by the above congruence,

$$\sum_{0 \leqslant m_1 < m_2'} \binom{m_2'}{m_1}(-1)^{m_1} + (-1)^{m_2'}(a_0/b_0)^{m_2'} u_{m_2'} \equiv 0 \pmod{\pi}.$$

By $\sum_{0\leqslant m_1\leqslant m_2'}\binom{m_2'}{m_1}(-1)^{m_1}=0$,

$$-(-1)^{m_2'}+(-1)^{m_2'}(a_0/b_0)^{m_2'}u_{m_2'}\equiv 0 \pmod{\pi},$$

hence

$$u_{m_2'}\equiv (b_0/a_0)^{m_2'} \pmod{\pi},$$

which is the desired result. We note $m_2'\leqslant p-2$ as $p-1\geqslant i>m_2'(=i-m_2)$ by $m_2>0$. For $i=p-1$, $m_2'\leqslant p-2$ and $u_{p-2}\equiv (b_0/a_0)^{p-2} \pmod{\pi}$ for $m_2'=p-2$. In the rest of this section, we assume $p>3$, from which we can take m_2' with $m_2'-2\geqslant 1$ and let $j=m_2'-2$ ($\geqslant 1$). Then by $n=l-m_2-m_1=0$, $r(j-i+l)=r(m_2'-2-i+i-m_2'+m_1)=r(m_1-2)$. As in the above, we have

$$\sum_{2\leqslant m_1\leqslant m_2'}\binom{i-m_2}{m_1}(-1)^{m_1}(a_0/b_0)^{m_1}u_{m_1-2}+\binom{i-m_2}{0}(-1)^0(a_0/b_0)^0u_{p-2}$$
$$+\binom{i-m_2}{1}(-1)(a_0/b_0)u_{p-1}\equiv 0 \pmod{\pi}.$$

By the above congruences of $u_{m_2'}$ for $m_2'=i-2$ with (12),

$$\sum_{2\leqslant m_1\leqslant m_2'}\binom{m_2'}{m_1}(-1)^{m_1}(a_0/b_0)^{m_1}(b_0/a_0)^{m_1-2}+\binom{m_2'}{1}(-1)(a_0/b_0)^2+u_{p-2}\equiv 0 \pmod{\pi}.$$

Therefore $(a_0/b_0)^2(-1)+u_{p-2}\equiv 0 \pmod{\pi}$, so $u_{p-2}\equiv (a_0/b_0)^2 \pmod{\pi}$. Hence

$$(b_0/a_0)^{p-2}\equiv (a_0/b_0)^2 \pmod{\pi} \quad\text{and}\quad b_0^p\equiv a_0^p \pmod{\pi},$$

by which $b_0=a_0$. Then we have the following theorem.

Theorem 3. *Let $p\geqslant 5$ and let $K=k(\alpha,\beta)$ be a Kummer extension of degree p^2 with $\mathrm{val}_K(\alpha-1)=p^2e_0-p$ and $\mathrm{val}_K(\beta)=p$. Let $G=\langle\sigma,\tau\rangle$ be an elementary abelian group of order p^2 such that $\sigma(\alpha)=\theta\alpha$, $\tau(\alpha)=\alpha$, $\sigma(\beta)=\beta$ and $\tau(\beta)=\theta\beta$. Let $a=a_0\pi^{e_0-1}$ be as above. Let K' be a Kummer extension with $Gal(K'/k)=G$. Then $\mathfrak{O}_{K'}\cong\mathfrak{O}_K$ if and only if there exist Kummer elements α',β' of K' such that $\mathrm{val}_{K'}(\alpha'-1)=p^2e_0-p$, $\mathrm{val}_{K'}(\beta')=p$, $\sigma(\alpha')=\theta\alpha'$, $\tau(\alpha')=\alpha'$, $\sigma(\beta')=\beta'$, $\tau(\beta')=\theta\beta'$, $\mathrm{val}_{K'}(\alpha'-1-a(\beta')^{p-1})=p^2e_0-1$ and $(\beta')^p\equiv\beta^p \pmod{\pi^2}$.*

Proof. We have just proved the part of 'only if' in the above and now prove the part of 'if'. Putting $u_{pm+r(j-i+l)}=1$, we have the left-hand side of the congruence of (6) is

$$\sum_{0\leqslant l\leqslant i}\binom{i}{l}(-1)^{i-l}a^{i-l}\pi^{i-l}v^{i-l-\delta_{i-j-l}}(\alpha-1)^l\beta^{j-i+l}.$$

As $(a\pi)^{i-l}\pi(\alpha-1)^l\beta^{j-i+l}\equiv 0 \pmod{\pi^{ie_0-\delta_{1-j}}}$ and $v\equiv(\beta'/\beta)^p\equiv 1 \pmod{\pi}$ by the assumptions,

$$\sum_{0\leqslant l\leqslant i}\binom{i}{l}(-1)^{i-l}a^{i-l}\pi^{i-l}v^{i-l-\delta_{i-j-l}}(\alpha-1)^l\beta^{j-i+l}$$
$$\equiv\sum_{0\leqslant l\leqslant i}\binom{i}{l}(-1)^{i-l}a^{i-l}\pi^{i-l}(\alpha-1)^l\beta^{j-i+l}\pmod{\pi^{ie_0-\delta_{1-j}}}.$$

Noting $a^{i-l}\pi^{i-l}\beta^{j-i+l}=(a\beta^{p-1})^{i-l}\beta^j$ by $\pi=\beta^p$, we can verify the congruences (6) hold. Hence $\mathfrak{O}_{K'}$ and $\mathfrak{O}_K$ are $\mathfrak{o}G$-isomorphic through the isomorphism Φ defined by $\Phi((\alpha')^i(\beta')^j)=\alpha^i\beta^j$. □

Here we give two examples. Let $k=\mathbb{Q}_5(\theta_5)$, $\alpha=\alpha'=\sqrt[5]{1+\pi^4}$, $\beta=\sqrt[5]{\pi}$ and $\beta'=\sqrt[5]{1+\pi}\sqrt[5]{\pi}$, where θ_5 is a primitive 5th root of 1. We remark $e_0=1$ and $k(\alpha,\beta)\neq k(\alpha',\beta')$.

$$\alpha^5\equiv\left(1+\beta^4\right)^5\equiv\left(1+(\beta')^4\right)^5\pmod{\pi^5}.$$

By [8, Theorem 1] with $\mathrm{val}_K(5)/4=25e_0$, $\mathrm{val}_K(\alpha-1-\beta^4)>25e_0-5$ and $\mathrm{val}_{K'}(\alpha'-1-(\beta')^4)>25e_0-5$ and $(\beta')^5\equiv\beta^5\pmod{\pi^2}$, whence $\mathfrak{O}_{K'}\cong\mathfrak{O}_K$ by $\Phi((\alpha')^i(\beta')^j)=\alpha^i\beta^j$.

Next let ω be a primitive 4th root of 1, $\omega_0=\sqrt[5]{\omega}$, $\alpha'=\sqrt[5]{1+\omega\pi^4}$ and $\beta'=\sqrt[5]{\pi}$. Let α,β be as above. Then

$$(\alpha')^5\not\equiv\left(1+(\beta')^4\right)^5\pmod{\pi^5}\quad\text{and}\quad(\alpha')^5\equiv\left(1+\omega_0(\beta')^4\right)^5\pmod{\pi^5}$$

and so $\mathrm{val}_K(\alpha'-1-\omega_0(\beta')^4)>25e_0-5$. We see $k(\alpha)\neq k(\alpha')$ and $K'\neq K$. By Theorem 3, we have $\mathfrak{O}_{K'}\not\cong\mathfrak{O}_K$.

Elder and Madan [3] give the decomposition of $\mathfrak{O}_K$ into indecomposable $\mathbb{Z}_pG$-modules when the first ramification number is one. From their results, it follows that if K' and K have the same second ramification number, then $\mathfrak{O}_{K'}\cong\mathfrak{O}_K$ as $\mathbb{Z}_pG$-modules. Theorem 3 implies that if $b_0\neq a_0$, then $\mathfrak{O}_{K'}$ and $\mathfrak{O}_K$ are $\mathbb{Z}_pG$-isomorphic but not $\mathfrak{o}G$-isomorphic. In [5, Corollary 2], we obtained the similar result there are cyclic Kummer extensions K/k and K'/k of degree p^2 such that $\mathfrak{O}_{K'}$ and $\mathfrak{O}_K$ are $\mathbb{Z}_pG$-isomorphic but not $\mathfrak{o}G$-isomorphic.

3. Free modules

In this section, we obtain conditions for $\mathfrak{O}_K$ to be $\mathfrak{A}$-free and give extensions such that $\mathfrak{O}_K$ are not $\mathfrak{A}$-free. Let $K=k(\alpha,\beta)$ be a totally ramified elementary abelian extension of degree p^2 over k as above. We further assume that the Kummer element β is a one-unit and $\mathrm{val}_K(\alpha-1-\sum_{0\leqslant l<p}a_l(\beta-1)^l)=p^2e_0-c_1(k(\alpha)/k)$ for some elements $a_0,a_1,\dots,a_{p-1}$ of $\pi\mathfrak{o}$. By the proof of Theorem 2, we see this assumption is satisfied in the case $(p-1)\,\mathrm{val}_K(\beta-1)<\mathrm{val}_K(\alpha-1)$. Let $\mathfrak{A}=\mathrm{End}_{\mathfrak{o}G}(\mathfrak{O}_K)$ and for $0\leqslant h<p^2$, let e_h be a primitive idempotent of kG such that $e_h(\alpha^i\beta^j)=\alpha^i\beta^j$ for $h=pi+j$ and $e_h(\alpha^i\beta^j)=0$ for $h\neq pi+j$, respectively. The maximal order $\mathfrak{M}$ in kG is equal to $\sum_h\mathfrak{o}e_h$. Let $\eta=(\alpha-1-\sum_l a_l(\beta-1)^l)^{p-1}(\beta-1)^{p-1}$, then clearly $K=kG\eta$. Define elements f_{pi+j} of $\mathfrak{M}$ by $f_{pi+j}\eta=(\alpha-1-\sum_l a_l(\beta-1)^l)^i(\beta-1)^j$. Further define elements $g_{pi+j}\in\mathfrak{M}$ by $g_{pi+j}(\sum_{0\leqslant l,m<p}\alpha^l\beta^m)=(\alpha-1-\sum_l a_l(\beta-1)^l)^i\times(\beta-1)^j$.

Lemma 3. *Let $g_{p^2-1}=\sum_{0\leqslant h<p^2}v_{h\ p^2-1}e_h$, then the elements $v_{h\ p^2-1}$ are units of $\mathfrak{o}$ and g_{p^2-1} is a unit of $\mathfrak{M}$.*

Proof. By the assumption $a_i \in (\pi)$,

$$\eta \equiv (\alpha-1)^{p-1}(\beta-1)^{p-1} \equiv \sum_{l,m} \alpha^l \beta^m \pmod{\pi \mathfrak{o}[\alpha,\beta]}.$$

Then $v_{h\ p^2-1} \equiv 1 \pmod{\pi}$, so $v_{h\ p^2-1}$ is a unit of $\mathfrak{o}$ and g_{p^2-1} is a unit of $\mathfrak{M}$. □

Let $f_{pi+j} = \sum_{0\leqslant h\leqslant p^2-1} b_{h\ pi+j} e_h$ with $b_{h\ pi+j} \in \mathfrak{o}$ and $g_{pi+j} = \sum_{0\leqslant h\leqslant p^2-1} v_{h\ pi+j} e_h$ with $v_{h\ pi+j} \in \mathfrak{o}$. Then

$$\left(\alpha - 1 - \sum_{0\leqslant l<p} a_l(\beta-1)^l\right)^i (\beta-1)^j = f_{pi+j}\eta = f_{pi+j} g_{p^2-1}\left(\sum_{l,m} \alpha^l \beta^m\right),$$

so $g_{pi+j} = f_{pi+j} g_{p^2-1}$. By the definition of g_{pi+j}, $v_{h,pi+j} = 0$ for $h > pi+j$, so $b_{h,pi+j} = 0$ for $h > pi+j$. Moreover, observing $v_{pi+j\ pi+j} = 1$, we have

$$b_{h\ pi+j} v_{h\ p^2-1} = v_{h\ pi+j} \text{ and particularly } b_{pi+j\ pi+j} v_{pi+j\ p^2-1} = 1. \tag{13}$$

By Proposition 1, $\mathfrak{O}_K = \sum_{pi+j} \mathfrak{o} f_{pi+j}\eta/\pi^{d_{pi+j}}$. Let $d'_{pi+j} = d_{p^2-1} - d_{pi+j}$ and $M = \sum_{pi+j} \mathfrak{o}\pi^{d'_{pi+j}} f_{pi+j}$. Then $\pi^{d'_{pi+j}} f_{pi+j}\eta/\pi^{d_{p^2-1}} = f_{pi+j}\eta/\pi^{d_{pi+j}}$, so $M\eta/\pi^{d_{p^2-1}} = \mathfrak{O}_K$. Remarking $d'_{p^2-1} = 0$ and $f_{p^2-1} = 1$, we have $1 \in M$. As $f_{pi+j} \in \mathfrak{M}$ and $d'_{pi+j} \geqslant 0$, $\pi^{d'_{pi+j}} f_{pi+j} \in \mathfrak{M}$ and so $M \subseteq \mathfrak{M}$. Since $\mathfrak{A}$ is the ring of $\mathfrak{o}G$-endomorphisms of M and $f_{p^2-1} = 1$, we have $\mathfrak{A} \subseteq M \subseteq \mathfrak{M}$. According to the arguments given in [6, Section 2], we seek the conditions for $\mathfrak{O}_K$ to be $\mathfrak{A}$-free. We can easily prove

Proposition 4. *$\mathfrak{O}_K$ is $\mathfrak{A}$-free if and only if M is an $\mathfrak{o}$-algebra.*

Let B be a $(p^2 \times p^2)$-matrix $(b_{h\ pi+j})$, then B is upper triangular, because $b_{h\ pi+j} = 0$ for $h > pi+j$. As $v_{h\ p^2-1}$ is a unit of $\mathfrak{o}$ by Lemma 3, it follows from (13) that $b_{pi+j\ pi+j}$ is a unit of $\mathfrak{o}$, hence B is an invertible matrix. Let $B^{-1} = (b'_{h\ pi+j})$. We see that M is an $\mathfrak{o}$-algebra if and only if for $0 \leqslant l \leqslant m < p^2$, generators $\pi^{d'_l} f_l$ and $\pi^{d'_m} f_m$ satisfy $\pi^{d'_l} f_l \pi^{d'_m} f_m \in M$. Moreover we note there exist elements $b^n_{l\ m}$ of k $(0 \leqslant l, m, n < p^2)$ such that

$$\pi^{d'_l} f_l \pi^{d'_m} f_m = \sum_{0\leqslant n<p^2} b^n_{l\ m} \pi^{d'_n} f_n.$$

Then $(\pi^{d'_l} f_l \pi^{d'_m} f_m) e_h = (\sum_{0\leqslant n<p^2} b^n_{l\ m} \pi^{d'_n} f_n) e_h$, so

$$\pi^{d'_l} b_{h\ l} \pi^{d'_m} b_{h\ m} = \sum_{h\leqslant n<p^2} b_{h\ n} b^n_{l\ m} \pi^{d'_n}. \tag{14}$$

Theorem 4. *Let K/k be as above and assume there exist elements a_l of (π) such that $\mathrm{val}_K(\alpha - 1 - \sum_l a_l(\beta-1)^l) = p^2 e_0 - c(k(\alpha)/k)$. Let $B = (b_{h\ l})$ and $B^{-1} = (b'_{h\ l})$ be as above. Then $\mathfrak{O}_K$ is $\mathfrak{A}$-free if and only if for $0 \leqslant h \leqslant l \leqslant m < p^2$,*

$$\mathrm{val}_k\left(\sum_{h\leqslant n\leqslant l} b'_{h\ n} b_{n\ l} b_{n\ m}\right) + d'_l + d'_m - d'_h \geqslant 0.$$

Proof. Using the inverse B^{-1}, we solve the linear equations (14) for $b^n_{l\,m}$ and so have

$$\pi^{d'_h} b^h_{l\,m} = \sum_{h\leqslant n\leqslant l} b'_{h\,n} b_{n\,l} b_{n\,m} \pi^{d'_l + d'_m}.$$

Then $b^h_{l\,m} \in \mathfrak{o}$ if and only if

$$\mathrm{val}_k\Bigg(\sum_{h\leqslant n\leqslant l} b'_{h\,n} b_{n\,l} b_{n\,m} \Bigg) + d'_l + d'_m - d'_h \geqslant 0,$$

which completes the proof of Theorem 4. □

In the following, we write $\mathrm{val}_K(\alpha - 1) = p^2 x - pr$ and $\mathrm{val}_K(\beta - 1) = p^2 y + pr'$ with $0 < r, r' < p$. Then there is an integer l_0 with $0 < l_0 < p$ such that

$$\mathrm{val}_K(\alpha - 1) \equiv l_0 \,\mathrm{val}_K(\beta - 1) \pmod{p^2}.$$

Since $\mathrm{val}_K(\alpha - 1) - l_0 \,\mathrm{val}_K(\beta - 1) = p^2(x - l_0 y) - p(r + l_0 r')$, it follows that for some integer $z > 0$, $r + l_0 r' = pz$. In the rest of this section, we assume

$$\mathrm{val}_k(a_l) > \mathrm{val}_k(a_{l_0}) \quad \text{for } l \neq l_0. \tag{15}$$

Set $a = a_{l_0}$ for brevity. Then

$$0 < \mathrm{val}_k(a) = x - l_0 y - z < e_0 < (p-1)e_0 = \mathrm{val}_k(p), \tag{16}$$

because $\mathrm{val}_K(\alpha - 1) < p^2 e_0$. Then, by (15), we can easily verify the next lemma.

Lemma 4. $(\alpha - 1 - \sum_l a_l(\beta-1)^l)^i (\beta-1)^j \equiv (\alpha-1)^i(\beta-1)^j + (\alpha-1)^{i-1} i(-1)a(\beta-1)^{l_0+j}$ $(\mathrm{mod}\ a\pi\,\mathfrak{o}[\alpha,\beta])$. *Moreover* $\eta \equiv (\alpha-1)^{p-1}(\beta-1)^{p-1} \equiv \sum_{0\leqslant i,j<p} \alpha^i \beta^j \pmod{a\pi\,\mathfrak{o}[\alpha,\beta]}$.

By Lemma 4, $v_{h,p^2-1} \equiv 1 \pmod{a\pi\,\mathfrak{o}[\alpha,\beta]}$. Then, by the definition of $b_{h\ pi+j}$ with (13), we observe, for $h = pm + n$ with $0 \leqslant m, n < p$,

$$\begin{aligned} b_{pm+n\ pi+j} \equiv{}& \binom{i}{m}(-1)^{i-m}\binom{j}{n}(-1)^{j-n} \\ &+ \binom{i-1}{m}(-1)^{i-1-m} i(-1)a\binom{l_0+j}{n}(-1)^{l_0+j-n} \pmod{a\pi\,\mathfrak{o}}. \end{aligned} \tag{17}$$

Moreover, we note if $l_0 + j \geqslant p$, then, for $n \neq 0$, $\binom{l_0+j}{n} \equiv 0 \pmod{a\pi\,\mathfrak{o}}$.

Now, to prove Theorem 5 stated later, we take $h = 1$, $l = p$, $m = (p-1)p + p - l_0$ or $h = 0$, $l = 2p$, $m = (p-2)p + p - 1$ for h, l, m given in Theorem 4. Write $e_0 - x$ in the form $e_0 - x = p[\frac{e_0 - x}{p}] + r''$ with $0 \leqslant r'' < p$. Then we have

$$p^2 e_0 - c_1 = p^2 e_0 - p(e_0 - x) - r = p^2\left(e_0 - \left[\frac{e_0 - x}{p}\right]\right) - pr'' - r.$$

Lemma 5. *Assume $c_1 > 2p$. Then*

$$d_p + d_{p(p-1)+p-l_0} - d_{p^2-1} - d_1 > \mathrm{val}_k(a).$$

Moreover, if $l_0 = 1$, then

$$d_{2p} + d_{p(p-2)+p-1} - d_{p^2-1} - d_0 > \mathrm{val}_k(a).$$

Proof. We first observe $c_1 > 2p$ if and only if $e_0 - x > 1$ and have

$$\begin{aligned} d_{pi+j} &= \left[\frac{i(p^2e_0 - c_1) + j\,\mathrm{val}_K(\beta - 1)}{p^2}\right] \\ &= i\left(e_0 - \left[\frac{e_0 - x}{p}\right]\right) + jy + \left[\frac{-i(pr'' + r) + jpr'}{p^2}\right]. \end{aligned}$$

Then $d_{p(p-1)+p-l_0} - d_{p^2-1} = [\frac{\mathrm{res}_2(pr''+r-pr-pr')-(l_0-1)p^2y-(l_0-1)pr'}{p^2}]$ and $d_p = (e_0 - [\frac{e_0-x}{p}] - 1) + [\frac{p^2-pr''-r}{p^2}]$, where $\mathrm{res}_2(x)$ denotes the remainder on dividing x by p^2.

$$\begin{aligned} &d_p + d_{p(p-1)+p-l_0} - d_{p^2-1} - d_1 \\ &\quad = e_0 - \left[\frac{e_0 - x}{p}\right] - 1 - l_0y - \left[\frac{l_0r'}{p}\right] \\ &\qquad + \left[\frac{\mathrm{res}_2(p(r'' - r - r') + r) + pr' - \mathrm{res}_2(l_0pr')}{p^2}\right] + y - y \\ &\quad = e_0 - x - \left[\frac{e_0 - x}{p}\right] - 1 + x - l_0y - z + 1 \\ &\qquad + \left[\frac{\mathrm{res}_2(p(r'' - r - r') + r) - p^2 + pr + pr'}{p^2}\right], \end{aligned}$$

because $l_0pr' = -pr + p^2z$. Therefore, by (16),

$$\begin{aligned} &d_p + d_{p(p-1)+p-l_0} - d_{p^2-1} - d_1 - \mathrm{val}_k(a) \\ &\quad = (p-1)\left[\frac{e_0 - x}{p}\right] + r'' + \left[\frac{\mathrm{res}_2(p(r'' - r - r') + r) - p^2 + pr + pr'}{p^2}\right]. \end{aligned}$$

By the assumption $c_1 > 2p$, we have $e_0 - x > 1$ and

$$(p-1)\left[\frac{e_0 - x}{p}\right] + r'' + \left[\frac{\mathrm{res}_2(p(r'' - r - r') + r) - p^2 + pr + pr'}{p^2}\right] > 0.$$

Hence the first inequality of Lemma 5 holds.

To verify the second inequality, we note $z = 1$ and $r + r' = p$ by the assumption $l_0 = 1$. Then $\mathrm{val}_k(a) = x - y - 1$. As in the above,

$$
\begin{aligned}
&d_{2p} + d_{p(p-2)+p-1} - d_{p^2-1} - d_0 \\
&\quad = 2\left(e_0 - \left[\frac{e_0 - x}{p}\right]\right) + \left[\frac{-2(pr'' + r)}{p^2}\right] + (p-2)\left(e_0 - \left[\frac{e_0 - x}{p}\right]\right) + (p-1)y \\
&\qquad + \left[\frac{-(p-2)(pr'' + r) + (p-1)pr'}{p^2}\right] - (p-1)\left(e_0 - \left[\frac{e_0 - x}{p}\right]\right) - (p-1)y \\
&\qquad - \left[\frac{-(p-1)(pr'' + r) + (p-1)pr'}{p^2}\right] \\
&\quad = e_0 - \left[\frac{e_0 - x}{p}\right] + \left[\frac{-2(pr'' + r)}{p^2}\right] \\
&\qquad + \left[\frac{\mathrm{res}_2(-(p-1)(pr'' + r) + (p-1)pr') + (pr'' + r)}{p^2}\right] \\
&\quad = e_0 - \left[\frac{e_0 - x}{p}\right] + \left[\frac{-2(pr'' + r)}{p^2}\right] + \left[\frac{\mathrm{res}_2(pr'' + r) + (pr'' + r)}{p^2}\right] \\
&\quad = (p-1)\left[\frac{e_0 - x}{p}\right] + r'' + x - y - 1 + y + 1 - 1 \\
&\quad = \mathrm{val}_k(a) + (p-1)\left[\frac{e_0 - x}{p}\right] + r'' + y > \mathrm{val}_k(a),
\end{aligned}
$$

because $e_0 - x > 1$ by the assumption $c_1 > 2p$. Hence the second inequality of Lemma 5 holds and the proof of Lemma 5 is completed. □

Here let S be the $(p^2 \times p^2)$-matrix $(s_{pm+n\ pi+j})$ as follows:

$$
S = (s_{pm+n\ pi+j}) \quad \text{with } s_{pm+n\ pi+j} = \binom{pi + j}{pm + n}(-1)^{pi+j-pm-n}
$$

for $0 \leqslant pm + n \leqslant pi + j$ and $s_{pm+n\ pi+j} = 0$ for $pi + j < pm + n$. Denote $\binom{i}{m}(-1)^{i-m}$ by $s_{m,i}$ and $\binom{i}{m}$ by $s'_{m,i}$. Then we see $s_{pm+n\ pi+j} \equiv s_{m,i}s_{n,j} \pmod{p\mathfrak{o}}$ and S is an invertible matrix. As in [6, Appendix],

$$
S^{-1} = (s'_{pm+n\ pi+j}) \quad \text{with } s'_{pm+n\ pi+j} = \binom{pi + j}{pm + n}
$$

for $0 \leqslant pm + n \leqslant pi + j$ and $s'_{pm+n\ pi+j} = 0$ for $pi + j < pm + n$. Put $B = S + aT$. Then we have $(S^{-1}T)^{p^2} = 0$ and

$$
B^{-1} = \left(I + aS^{-1}T\right)^{-1}S^{-1} = S^{-1} - aS^{-1}TS^{-1} + a^2\left(S^{-1}T\right)^2S^{-1} + \cdots. \tag{18}
$$

By (17),

$$
t_{pm+n\ pi+j} \equiv s_{m,i-1}i(-1)s_{n,l_0+j} \pmod{\pi\mathfrak{o}},
$$

so that

$$b_{pm+n\ pi+j} \equiv s_{m,i}s_{n,j} + s_{m,i-1}i(-1)s_{n,l_0+j}a \pmod{a\pi\mathfrak{o}}$$

and

$$b'_{pm+n\ pi+j} \equiv s'_{m,i}s'_{n,j} - \Bigl(\sum s'_{m,\gamma}s'_{n,\delta}s_{\gamma,\mu-1}\mu(-1)s_{\delta,l_0+\nu}s'_{\mu,i}s'_{\nu,j}\Bigr)a \pmod{a\pi\mathfrak{o}},$$

where the sum runs over $pm+n \leqslant p\gamma+\delta \leqslant p\mu+\nu \leqslant pi+j$.

We evaluate the sum $\sum_{1\leqslant n\leqslant p} b'_{1,n}b_{n,p}b_{n,p(p-1)+p-l_0}$. By Lemma 4 with (18), we have for $n = pn_1+n_0$,

$$\begin{aligned} b'_{1,\,pn_1+n_0} \equiv{}& s'_{0,n_1}s'_{1,n_0} - \sum s'_{0,h_1}s'_{1,h_0}\binom{m_1-1}{h_1}(-1)^{m_1-1-h_1}m_1(-1) \\ &\times \binom{l_0+m_0}{h_0}(-1)^{l_0+m_0-h_0}s'_{m_1,n_1}s'_{m_0,n_0}a \pmod{a\pi\mathfrak{o}}, \end{aligned}$$

where the sum runs over $1 \leqslant h_1p+h_0 \leqslant m_1p+m_0 \leqslant n_1p+n_0\ (< p^2)$. Moreover,

$$b_{n,p} \equiv s_{n_1,1}s_{n_0,0} + s_{n_1,1-1}(-1)s_{n_0,l_0+0}a \pmod{a\pi\mathfrak{o}}$$

and

$$b_{n,p(p-1)+p-l_0} \equiv s_{n_1,p-1}s_{n_0,p-l_0} + s_{n_1,p-2}(p-1)(-1)s_{n_0,l_0+p-l_0}a \pmod{a\pi\mathfrak{o}}.$$

As is easily known,

$$\sum_m s'_{h,m}s_{m,i}s_{m,u} = (-1)^{i+u}\binom{i}{h}\binom{i+u-h}{i}$$

(for example, cf. [6, (A.2)]). Then we have

$$\begin{aligned} &\sum_{1\leqslant n\leqslant p} b'_{1,n}b_{n,p}b_{n,p(p-1)+p-l_0} \\ &\quad\equiv \sum_{1\leqslant pn_1+n_0\leqslant p} s'_{0,n_1}s_{n_1,1}s_{n_1,p-1}s'_{1,n_0}s_{n_0,0}s_{n_0,p-l_0} \\ &\qquad+\Bigl(\sum_{1\leqslant pn_1+n_0\leqslant p} s'_{0,n_1}s_{n_1,1-1}(-1)s_{n_1,p-1}s'_{1,n_0}s_{n_0,l_0+0}s_{n_0,p-l_0}\Bigr)a \\ &\qquad+\Bigl(\sum_{1\leqslant pn_1+n_0\leqslant p} s'_{0,n_1}s_{n_1,1}s_{n_1,p-2}s'_{1,n_0}s_{n_0,0}s_{n_0,l_0+p-l_0}\Bigr)a \\ &\qquad-\Bigl(\sum_{1\leqslant ph_1+h_0\leqslant pm_1+m_0\leqslant pn_1+n_0\leqslant p} \bigl(s'_{0,h_1}s_{h_1,m_1-1}m_1(-1)s'_{m_1,n_1}s_{n_1,1}s_{n_1,p-1} \end{aligned}$$

$$\cdot s'_{1,h_0}s_{h_0,l_0+m_0}s'_{m_0,n_0}s_{n_0,0}s_{n_0,p-l_0}\Big)\Big)a$$
$$\equiv 0-(-1)^{l_0+p-l_0}\binom{l_0}{1}\binom{p-1}{l_0}a+0+s_{1,p-1}\Big(\sum_{1\leqslant h_0\leqslant l_0}s'_{1,h_0}s_{h_0,l_0}\Big)s_{0,p-l_0}a$$
$$\equiv\big((-1)^{l_0}l_0+\delta_{1,l_0}(-1)^{p-l_0}\big)a \pmod{a\pi\mathfrak{o}},$$

because $s'_{1,n_0}s_{n_0,0}=0$ and $\mathrm{val}_k(a)<\mathrm{val}_k(p)$ by (16). We can prove the next theorem which is one of the main results of this paper.

Theorem 5. *Let $K=k(\alpha,\beta)$ be a totally ramified elementary abelian Kummer extension of degree p^2 such that the first ramification numbers $c(k(\alpha)/k)$, $c(k(\beta)/k)$ are prime to p. Let elements a_l of $\pi\mathfrak{o}$ and l_0 be as above. Assume $\mathrm{val}_k(a_{l_0})<\mathrm{val}(a_l)$ for $l\neq l_0$ and $c_1>2p$. Moreover, assume $p\geqslant 5$ in case $l_0=1$. Then $\mathfrak{O}_K$ is not $\mathfrak{A}$-free.*

Proof. We first consider the case $l_0>1$. Then $\delta_{1,l_0}=0$. By Lemma 5 and the above congruence,

$$\mathrm{val}_k\Big(\sum_{1\leqslant n\leqslant p}b'_{1,n}b_{n,p}b_{n,p(p-1)+p-l_0}\Big)+d'_p+d'_{p(p-1)+p-l_0}-d'_1$$
$$=\mathrm{val}_k(a)-(d_p+d_{p(p-1)+p-l_0}-d_{p^2-1}-d_1)<0.$$

By Theorem 4, we have $\mathfrak{O}_K$ is not $\mathfrak{A}$-free.

Next we consider the case $l_0=1$ and take $h=0$, $l=2p$, $m=p(p-2)+p-1$ for h,l and m given in Theorem 4. By the assumption $p>3$, $l<m$. As in the case considered above, we have

$$\sum_{0\leqslant n\leqslant 2p}b'_{0,n}b_{n,2p}b_{n,p(p-2)+p-1}$$
$$\equiv\sum_{0\leqslant pn_1+n_0\leqslant 2p}s'_{0,n_1}s_{n_1,2}s_{n_1,p-2}s'_{0,n_0}s_{n_0,0}s_{n_0,p-1}$$
$$+\Big(\sum_{0\leqslant pn_1+n_0\leqslant 2p}s'_{0,n_1}s_{n_1,2-1}2(-1)s_{n_1,p-2}s'_{0,n_0}s_{n_0,1+0}s_{n_0,p-1}\Big)a$$
$$+\Big(\sum_{0\leqslant pn_1+n_0\leqslant 2p}s'_{0,n_1}s_{n_1,2}s_{n_1,p-3}(p-2)(-1)s'_{0,n_0}s_{n_0,0}s_{n_0,1+p-1}\Big)a$$
$$-\Big(\sum_{0\leqslant ph_1+h_0\leqslant pm_1+m_0\leqslant pn_1+n_0\leqslant 2p}\big(s'_{0,h_1}s_{h_1,m_1-1}m_1(-1)s'_{m_1,n_1}s_{n_1,2}s_{n_1,p-2}$$
$$\cdot s'_{0,h_0}s_{h_0,1+m_0}s'_{m_0,n_0}s_{n_0,0}s_{n_0,p-1}\big)\Big)a$$
$$\equiv 0+\Big(\sum_{n_1=0}s'_{0,0}s_{0,1}(-2)s_{0,p-2}s'_{0,n_0}s_{n_0,1}s_{n_0,p-1}\Big)a$$

$$
\begin{aligned}
&+\Bigg(\sum_{n_1=1} s'_{0,1}s_{1,1}(-2)s_{1,p-2}s'_{0,n_0}s_{n_0,1}s_{n_0,p-1}\Bigg)a\\
&+\Bigg(\sum_{0\leqslant pn_1+n_0\leqslant 2p} s'_{0,n_1}s_{n_1,2}s_{n_1,p-3}2s'_{0,0}s_{0,0}s_{0,1+p-1}\Bigg)a\\
&-\Bigg(\sum_{m_1=1} s'_{0,0}s_{0,0}(-1)s'_{1,n_1}s_{n_1,2}s_{n_1,p-2}s'_{0,h_0}s_{h_0,1}s'_{0,0}s_{0,0}s_{0,p-1}\\
&+\sum_{m_1=2} s'_{0,h_1}s_{h_1,1}2(-1)s'_{2,n_1}s_{n_1,2}s_{n_1,p-2}s'_{0,h_0}s_{h_0,1}s'_{0,0}s_{0,0}s_{0,p-1}\Bigg)a\\
&\equiv 2(-1)^{p-2}(-1)^{1+p-1}\binom{1}{0}\binom{p}{1}a+4(-1)^{p-2-1}(-1)^{1+p-1}\binom{1}{0}\binom{p}{1}a\\
&\quad+(-2)(-1)^{2+p-3}\binom{2}{0}\binom{p-1}{2}a\\
&\equiv -2a \pmod{a\pi\mathfrak{o}},
\end{aligned}
$$

because $\sum_{h_1} s'_{0,h_1}s_{h_1,1}=0$. Therefore, by Lemma 5, for $l_0=1$,

$$
\begin{aligned}
&\mathrm{val}_k\Bigg(\sum_{0\leqslant n\leqslant 2p} b'_{0,n}b_{n,2p}b_{n,p(p-2)+p-1}\Bigg)+d'_{2p}+d'_{p(p-2)+p-1}-d'_0\\
&\quad=\mathrm{val}_k(a)-(d_{2p}+d_{p(p-2)+p-1}-d_{p^2-1}-d_0)<0,
\end{aligned}
$$

from which it also follows that $\mathfrak{O}_K$ is not $\mathfrak{A}$-free. The proof of Theorem 5 is completed. □

Here we give an example. Let $k=\mathbb{Q}_5(\theta_{25})$, $\alpha=\sqrt[5]{1+\pi^9}$ and $\beta=\sqrt[5]{1+\pi}$. Then $l_0=4$, $a_4\in\pi\mathfrak{o}$ and $a_i\in\pi^2\mathfrak{o}$ for $0\leqslant i<4$, because $\mathrm{val}_K(a_i(\beta-1)^i)>\mathrm{val}_K(a_4(\beta-1)^4)$. Hence $\mathfrak{O}_K$ is not $\mathfrak{A}$-free.

Acknowledgment

The author thanks the referee for a lot of valuable advices.

References

[1] N.P. Byott, Tame and Galois extensions with respect to Hopf orders, Math. Z. 220 (1995) 495–522.
[2] J. Cassels, A. Fröhlich, Algebraic Number Theory, Academic Press, London, 1967.
[3] G.G. Elder, M.L. Madan, Galois module structure of the integers in wildly ramified $C_p\times C_p$ extensions, Canad. J. Math. 49 (4) (1997) 722–735.
[4] Y. Miyata, Wildly ramified extensions of prime degree p and Stickelberger conditions, Japan J. Math. 15 (1) (1989) 157–168.
[5] Y. Miyata, On the invariant factors of Kummer orders on the rings of integers of $\mathfrak{p}$-adic number fields of degree p^2, J. Number Theory 66 (2) (1997) 314–330.
[6] Y. Miyata, On the module structure of rings of integers in $\mathfrak{p}$-adic number fields over associated orders, Math. Proc. Cambridge Philos. Soc. 123 (1998) 199–212.
[7] J.P. Serre, Local Fields, Grad. Texts in Math., vol. 67, Springer-Verlag, Berlin, 1979.
[8] B.F. Wyman, Wildly ramified gamma extensions, Amer. J. Math. 91 (1969) 135–152.